

Abstract of the Disclosure

In order to prevent an illegal copy of an encoded digital content downloaded by users for reproduction, all systems connected to the users generate a plurality of keys which are mutually shared, and download and upload the digital content by using channels formed between units performing mutual communication.

A unit for supplying the digital content receives an authorization of legally supplying the digital content from an authorization recognition unit. The first content output unit is authenticated from the digital content supplying unit. At this time, the digital content supplying unit and the first content output unit form a sharing key to form a channel between the two. The second content output unit is authenticated from the digital content supply unit through the first content output unit, the first content output unit and the second content output unit form a channel to the channel key. The digital content between the first content output unit and the second output unit is downloaded and uploaded according to respective control state data of the first content output unit and the second output unit. Accordingly, the digital content transmitted between the digital content supply unit, the first content output unit, and the second content output unit can be prevented from an illegal copy. A system having a portable recordable medium for preventing an illegal copy of digital contents, and more particularly to a system having a portable recordable medium by using a physical address of bad sector formed the portable recordable medium during manufacturing process of the portable recordable medium and by encrypting a header of the encrypted digital contents stored in the portable recordable medium and recording the encrypted header on a physical address of bad sector of the portable recordable medium. The physical address of bad sector is formed on the portable recordable medium during manufacturing process of the portable recordable medium. This is for preventing an illegal copy of the downloaded digital contents through a terminal after the digital contents has been downloaded.

An illegal copy protecting system having a portable terminal transmitting the encrypted digital content which is received from digital content supply unit to a digital content storage medium. In another preferred embodiment, the digital content transmitted from LCM can be stored directly in the digital content storage medium. The system includes

a portable terminal processing the random number stored in spare area of the digital content storage medium such as physical address of the bad sector of the digital content storage medium and transmitting the encrypted header of the digital content by using the processed value of the random number, and a digital content storage medium reading and transmitting the physical address by using the portable terminal and storing the number as a key value randomly generated by the portable terminal, and storing the encrypted header information encrypted by the resultant value and the encrypted digital content as sector data